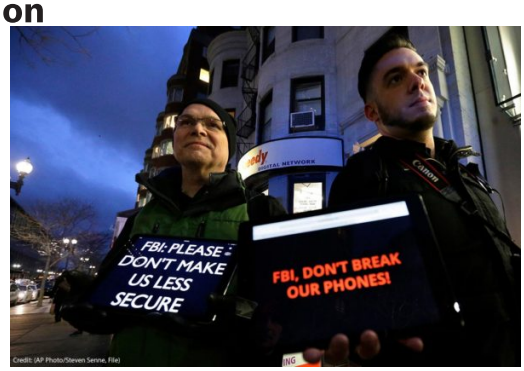
NEWS & COMMENTARY



In Latest Encryption Battle with Apple, Justice Department Still Wrong

Law enforcement does not have the authority to commandeer third parties into becoming its undercover agents or hackers.

Jennifer Stisa Granick,
Surveillance and Cybersecurity Counsel

January 23, 2020

The federal government is once again trying to force Apple to weaken the security of millions of iPhones. On Wednesday, President Trump issued a call from Davos, Switzerland for Apple to assist law enforcement in unlocking iPhones. Last week, Trump made the same demand of Apple, tweeting that the company should unlock cell phones as a quid pro quo for any benefits it enjoys as a result of favorable U.S. trade deals.

Buying off private parties to do police bidding is neither good trade policy nor good law enforcement. Regardless, President Trump's attorney general, William Barr, has made this fight one of his signature issues. In July and October of last year, he gave speeches

that pushed for tech companies to design their products to ensure law enforcement access to our secured communications. This month he initiated a public spat with Apple, criticizing the company for failing to unlock the Pensacola shooter's iPhone.

But there is considerable global demand that communications software provide strong encryption to protect users — and for good reason. Encryption is our strongest defense against abusive governments, hackers, and organized crime. Encryption also provides anonymity to dissidents, whistleblowers, and human-rights defenders so they can freely express themselves, organize, and expose governmental abuse without fear of retribution.

Requiring technology companies to build a government backdoor into our encrypted

communications would break that crucial defense, empowering repressive governments like China and Iran to obtain and abuse private communications.

This is not just about the Pensacola investigation, or any one criminal case. Satisfying the government's demand would undermine the security of millions of other iPhone users, and make them all more susceptible to government abuses, identity thieves, credit card fraud, and other criminal activity. If technology companies build security weaknesses into their products, unwanted attackers will use those weaknesses for crime and abuse.

This is why Apple went all in resisting the FBI's effort four years ago to unlock an iPhone (and the ACLU supported Apple), why Google rapidly deployed secure encryption across all

its data streams, and why Facebook is making end-to-end encryption the default on WhatsApp, Messenger, and Instagram.

But law enforcement and intelligence agencies have not given up. Attorney General Barr's public relations campaign implies that the Department of Justice will only seek information with a lawfully-issued search warrant. At the same time, the DOJ has been telling federal courts across the country that it does not need a search warrant to obtain our emails or other private data. Nor are all of the Department's search warrants legally justified. The FBI has been spying on Black Americans, including arresting and detaining one man for his First Amendment-protected Facebook posts.

Encryption providers have the law on their side. The Fourth Amendment

generally requires a search warrant before police can seize and read our private correspondence. A warrant gives police permission to search, but it doesn't entitle them to plaintext information that doesn't exist. Moreover, there is no law in the U.S. requiring individuals to ensure our private communications are available to law enforcement.

Technology providers also have a number of government agencies on their side. The Commerce and State Departments have argued internally that mandating encryption "backdoors" will have negative economic, security, and diplomatic consequences. The Federal Trade Commission, charged with protecting consumer privacy, pushes encryption as a means to secure consumer data from theft.

Former government officials are also pushing back on

DOJ's claims. Jim Baker, who was the FBI general counsel responsible for the agency's litigation against Apple, recently wrote that it was time to accept that end-to-end encryption is here to stay, citing in part the fact that "relevant cybersecurity risks to society have grown disproportionately over the years when compared with other risks." The former director of the National Security Agency and the Central Intelligence Agency, Michael Hayden, argues that encryption backdoors will empower authoritarian governments without helping law enforcement, as criminals will simply switch to services designed overseas.

Nevertheless, the Department of Justice has doubled down – often in secret and under sealed legal proceedings – on its efforts to compel device manufacturers and social networking companies to

undermine the security promises they make to us. For instance, in 2018, Reuters reported on a failed FBI attempt to force Facebook to wiretap encrypted voice conversations on Facebook Messenger. The public to date doesn't know exactly what the FBI demanded that Facebook change about Messenger, how that change might affect the security and privacy of other Messenger users, why the court denied the request, how many other times the FBI has made such a request, or how many other companies have received one. We also don't know who has complied with the government's requests in the past, or under what legal interpretation. The ACLU and EFF have sued to unseal the court opinion, and will be in court on April 3rd to argue that the law should be public in a democracy.

The government's attempts to force developers to build

insecure products, or to undermine existing security measures, as it is attempting to do with Apple right now, are dangerous and unlawful. Law enforcement does not and should not have the authority to commandeer innocent third parties into becoming its undercover agents, spies, or hackers. The Department of Justice and members of Congress should abandon attempts to undermine our security, and instead focus on policies that encourage widespread adoption of strong encryption. We should be leading the global community by example, making it clear that the United States supports and encourages secure infrastructure for our society, and that we consider excessive surveillance powers held by anyone a problem – not a solution.

STAY INFORMED

Sign up to be the first to hear about how to take action.

By completing this form, I agree to receive occasional emails per the terms of the ACLU's privacy policy.

First name

Last name

Email

ZIP code

By completing this form, I agree to receive occasional emails per the terms of the ACLU's privacy policy.

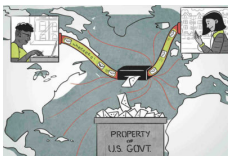
Sign up

More in Privacy & Technology

Apple and Google Announced a Coronavirus Tracking System. How Worried Should We Be?

Federal Court Rules That Border Officers Can't Arbitrarily Search Our Electronic Devices

Anti-Distracted Driving "Textalyzer" Technology: Not as Simple as it Seems



Victory! Court Allows Wikimedia's Challenge to NSA Surveillance to Go Forward

Search ACLU.org using DuckDuckGo

Contact us
Careers and internships
Shop **Donate**

User agreement

Privacy statement

Accessibility

Contact us
Careers and internships
Shop **Donate**

Search ACLU.org using DuckDuckGo